PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-325153
(43)Date of publication of application : 22.11.2001

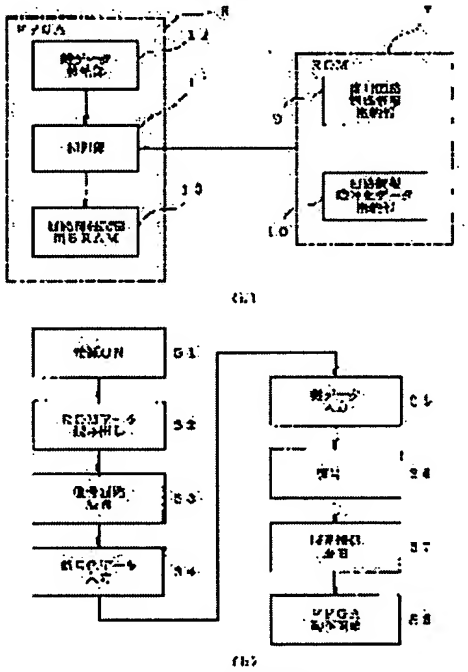
(51)Int.Cl. G06F 12/14
H04L 9/10

(21)Application number : 2000-142456
(22)Date of filing : 15.05.2000

(71)Applicant : TOYO COMMUN EQUIP CO LTD
(72)Inventor : KUROSAWA KAZUO

(54) CIRCUIT INFORMATION PROTECTING METHOD FOR FIELD PROGRAMMABLE GATE ARRAY

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a circuit information protecting method of an FPGA by which data of a ROM in which circuit information of the FPGA is written can be protected and use of the ROM by unauthorized copy can be prevented.
SOLUTION: The method is carried out by providing the ROM 7 to store the circuit information and the FPGA 8 as a user programmable integrated circuit, the ROM 7 is provide with a decoding circuit structure information storage part 9 and a circuit information encryption data storage part 10 and the FPGA 8 is provided with a control part 11 to control read and write of the data stored in the ROM 7 and the FPGA 8, a key data storage part 12 and an SRAM 13 for storing circuit information.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－325153
（P2001－325153A）
(43)公開日　平成13年11月22日(2001.11.22)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ｚ	５Ｊ１０４

審査請求　未請求　請求項の数３　ＯＬ　（全５頁）

(21)出願番号　特願2000－142456(P2000－142456)

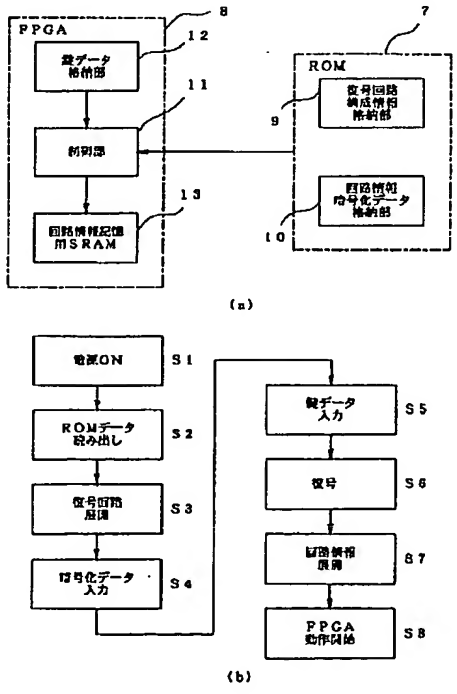
(22)出願日　平成12年５月15日(2000.5.15)

(71)出願人　000003104
東洋通信機株式会社
神奈川県高座郡寒川町小谷２丁目１番１号
(72)発明者　黒沢　和雄
神奈川県高座郡寒川町小谷二丁目１番１号
東洋通信機株式会社内

Ｆターム(参考)　5B017 AA03 AA06 BA07 CA11
5J104 AA47 JA03 NA02

(54)【発明の名称】　フィールドプログラマブルゲートアレイの回路情報保護方法

(57)【要約】
【課題】ＦＰＧＡの回路情報を書き込んだＲＯＭのデータを保護し、ＲＯＭを不正にコピーして使用することを防止できるＦＰＧＡの回路情報保護方法を提供することを目的とする。
【解決手段】回路情報を格納するＲＯＭ７と、ユーザがプログラム可能な集積回路であるＦＰＧＡ８とにより構成し、ＲＯＭ７には、復号回路構成情報格納部９と回路情報暗号化データ格納部１０とを備え、ＦＰＧＡ８には、ＲＯＭ７及び、ＦＰＧＡ８に格納したデータの読み出し及び書き込みを制御する制御部１１と鍵データ格納部１２と回路情報記憶用ＳＲＡＭ１３とを備えている。



1

【特許請求の範囲】
【請求項１】揮発性メモリを備えたフィールドプログラマブルゲートアレイに回路情報を書き込む手段として該フィールドプログラマブルゲートアレイ外部に不揮発性メモリを設け、該不揮発性メモリに回路情報を書き込み、電源投入時に前記不揮発性メモリからフィールドプログラマブルゲートアレイに備えた前記揮発性メモリに回路情報を書き込む方法において、
前記不揮発性メモリに書き込む回路情報を暗号化データとし、フィールドプログラマブルゲートアレイ上で暗号化データを復号したことを特徴とするフィールドプログラマブルゲートアレイの回路情報保護方法。
【請求項２】前記回路情報を保護する際に、フィールドプログラマブルゲートアレイ内部の外部から読み出し不可能な不揮発性メモリ領域に鍵データを格納し、復号時に使用したことを特徴とする請求項１記載のフィールドプログラマブルゲートアレイの回路情報保護方法。
【請求項３】前記回路情報を保護する際に、前記フィールドプログラマブルゲートアレイ外部に設けた回路情報を格納する前記不揮発性メモリに復号回路の構成情報と前記暗号化データとを格納したことを特徴とする請求項１記載のフィールドプログラマブルゲートアレイの回路情報保護方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はフィールドプログラマブルゲートアレイ（以降、ＦＰＧＡと称す）の回路情報保護方法に関し、特にＦＰＧＡの揮発性メモリ（以降、ＳＲＡＭと称す）領域に回路情報を記憶して動作するＦＰＧＡの回路情報保護方法に関する。
【０００２】
【従来の技術】ＦＰＧＡは、回路を構成する素子の位置や配線の情報を与えるプログラミングを行い入力することにより所望の論理回路を生成する集積回路である。即ち、ＦＰＧＡには、予め多数の汎用論理回路を格子状に配置した標準的なチップを備えており、ユーザは、所望の集積回路を実現するためＦＰＧＡに必要な所定の情報をプログラムし入力することによって、前記汎用論理回路の接続を行ない、所定の機能を備えた論理回路の生成を可能とする。そこで、ＦＰＧＡを採用することにより装置の設計、製造を短期間で行うことが出来ることから初期コストが少ない等、装置の開発を行う上で非常に有利となる。又、ＦＰＧＡを実現するものの一つとしてＳＲＡＭ方式のＦＰＧＡがあり、ＦＰＧＡ内部に設けられているＳＲＡＭ領域に、所望の集積回路を得るために必要な回路機能を定義する回路情報をプログラムして格納し、該プログラムに従って動作する。そこで、前記回路情報を電源切断時にも保持する必要が有り外部に不揮発性メモリ（以降、ＲＯＭと称す）を用意し、電源投入時に自動的に前記回路情報をＦＰＧＡにロードするようにしている。

2

【０００３】図４に従来から用いられているＳＲＡＭ方式ＦＰＧＡのチップ構成例を示す。ＦＰＧＡチップ１は、入出力ブロック２と、論理ブロック３と、スイッチマトリックス４とにより構成し、更にスイッチマトリックス４は、１ビットＳＲＡＭセル５と、ＦＥＴトランジスタ６とにより構成する。ＦＰＧＡの動作を説明すると、ＦＰＧＡが所望の機能を果たすように回路機能情報をプログラミングし、外部からＦＰＧＡのＳＲＡＭに書き込むことによりスイッチマトリックス４を制御し、論理ブロック３の機能を設定して複雑な論理演算を行う。入出力ブロック２は、外部への入出力ピンと論理ブロック３とのインタフェース手段であり、一般にトライステート制御可能なドライバーとレシーバーを備えている。論理ブロック３は、通常、複数の論理関数を備えた標準回路が用意され選択することが可能である。
【０００４】
【発明が解決しようとする課題】しかしながら、従来のＳＲＡＭ方式のＦＰＧＡは、回路情報を記憶しておくＲＯＭを用い、電源投入時にＲＯＭから回路情報をロードして使用しているが、このＲＯＭの内容は、ＲＯＭライタ等を使用することにより容易に第３者が読み取り可能であり、コピーしたＲＯＭを用いてＦＰＧＡの機能を不正使用することができる。又、ＲＯＭに書き込むデータの形式、ＦＰＧＡ-ＲＯＭ間のデータの転送方法を秘密にすることにより、秘密の漏洩を防止することは可能であるが、内容をコピーして使用することは防止できない。本発明は、上述したような従来のＳＲＡＭ方式のＦＰＧＡが抱えている問題点を解決するためになされたものであって、ＲＯＭに書き込んだ回路情報を保護しＲＯＭを不正にコピーして使用することを防止できるＦＰＧＡの回路情報保護方法を提供することを目的とする。
【０００５】
【課題を解決するための手段】上記目的を達成するために本発明に係るＦＰＧＡの回路情報保護方法は、以下の構成をとる。請求項１記載のＦＰＧＡの回路情報保護方法は、揮発性メモリを備えたフィールドプログラマブルゲートアレイに回路情報を書き込む手段である、外部に不揮発性メモリを設け該不揮発性メモリに回路情報を書き込み、電源投入時に前記不揮発性メモリからフィールドプログラマブルゲートアレイに備えた前記揮発性メモリに回路情報を書き込む方法において、前記不揮発性メモリに書き込む回路情報を暗号化データとし、フィールドプログラマブルゲートアレイ上で暗号化データを復号するよう構成する。請求項２記載のＦＰＧＡの回路情報保護方法は、前記回路情報を保護する際に、フィールドプログラマブルゲートアレイ内部の外部から読み出し不可能な不揮発性メモリ領域に鍵データを格納し、復号時に使用するよう構成する。請求項３記載のＦＰＧＡの回路情報保護方法は、前記回路情報を保護する際に、外部

に設けた回路情報を格納する前記不揮発性メモリに復号回路の構成情報と前記暗号化データとを格納するよう構成する。

【０００６】

【発明の実施の形態】以下、図示した実施例に基づいて本発明を詳細に説明する。先ず、本発明の実施例を示す前に、本発明に係る暗号化技術について説明する。暗号とは、情報の内容が当事者以外に知られないように情報を変換することをいい、送信側において暗号化鍵と呼ばれるパラメータにより情報を暗号文に変換し、受信側において復号鍵を用いて暗号文を元の情報に戻すことである。又、暗号化鍵と復号鍵との関係には、両者が同一であり片方から残りを容易に求められる暗号である共通鍵方式と、片方から残りを容易に求められない暗号である公開鍵方式がある。本実施例における暗号方式は、共通鍵方式を採用しており、以下共通鍵方式を説明する。共通鍵方式は、情報の送信側及び受信側が予め共通の鍵を共有しておき、この鍵を基に情報を暗号文に変換する方法である。共通鍵方式の特徴として暗号化処理の高速性が有り、任意の入力に対する暗号化出力への処理過程は十分小さく効率の良い方式である。共通鍵方式の具体例として知られているものとして、ＤＥＳ方式が有り、６４ビットのデータを５６ビットの鍵により暗号化し、鍵データは任意とするが一般的には乱数データを生成して、それを鍵としている。

【０００７】図２に共通鍵方式による暗号化処理の流れを示す。同図の流れを説明すると、先ず、送信側においては、機密保護を必要とする情報を定められたパラメータからなる暗号化鍵により、そのままでは意味を持たない暗号情報に変換する。暗号化鍵と受信側において使用する復号鍵は、前もって定めた共通のパラメータを持ち、共通鍵暗号とする。受信側においては、送信側に備えていた暗号化鍵に対応する復号鍵を所有しており、送られてきた暗号情報を復号鍵により復号する。一方、第三者が暗号情報を入手し暗号情報を復号しようとする行為である解読とは、復号鍵と同等の機能を備えたパラメータを数学的手段を用いて再現することで、その困難さが暗号系の安全性に係る。そこで、本実施例における暗号とは、回路情報が書き込まれているＲＯＭの内容が、第三者に知られないよう回路情報を何らかのパラメータに従った暗号化鍵により変換し、ＦＰＧＡにおいて、入力した暗号化されている回路情報をＦＰＧＡに備えた復号鍵により元のデータに復号するものである。

【０００８】図１は、本発明に係るＦＰＧＡの回路情報保護方法の一実施例を示す構成図であり、（ａ）にブロック構成例を、（ｂ）に処理の流れ図を示す。図１（ａ）を説明すると、同図は、回路情報を格納するＲＯＭ７と、ユーザがプログラム可能な集積回路であるＦＰＧＡ８とにより構成し、ＲＯＭ７には、復号回路構成情報格納部９と回路情報暗号化データ格納部１０とを備え、ＦＰＧＡ８には、ＲＯＭ７及び、ＦＰＧＡ８に格納したデータの読み出し及び書き込みを制御する制御部１１と鍵データ格納部１２と回路情報記憶用ＳＲＡＭ１３とを備えている。

【０００９】図１（ａ）の動作を説明すると、電源起動時に回路情報をＦＰＧＡ８に出力するＲＯＭ７には、復号回路構成情報格納部９に暗号化データを暗号化されていないデータに復号する操作を行うための復号演算を実行する回路のデータが、又、回路情報暗号化データ格納部１０には、ＦＰＧＡが機能する回路情報を暗号化したデータとが格納されている。そこで、電源を投入すると、ＦＰＧＡ８は、論理ゲート及びフリップフロップ等で構成する制御部１１の動作によりＲＯＭ７より復号回路構成情報を読み出し、読み出した復号回路をＦＰＧＡ８上に展開する。次に、ＲＯＭ７より回路情報暗号化データを読み出し、前記復号回路に入力して復号する。ＦＰＧＡ８では、ＲＯＭ７において回路情報を暗号化した際に使用した暗号化鍵に対応した鍵データを鍵データ格納部１２に備えており、復号する際に使用する。鍵データ格納部１２は、鍵データを第三者に読み出されると情報が漏れてしまうため、外部から鍵データを読み出すことができないよう鍵データ出力が外部出力用ピン等に接続されない構成をとる。そこで、復号回路により復号した回路情報は、回路情報記憶用ＳＲＡＭに記憶され所望の機能を備えたＦＰＧＡとして動作し、ＲＯＭ７に格納された回路情報は、第三者に対して十分機密保持可能となる。

【００１０】図１（ｂ）について説明する。同図は、本発明に係るＲＯＭからＦＰＧＡへのデータの読み出し手順を示す処理の流れ図である。ＦＰＧＡを搭載したシステムに電源を投入すると（ステップ１）、ＦＰＧＡは、制御回路を動作させＲＯＭよりデータを読み出す（ステップ２）。回路情報を復号するために、先ず、暗号演算を実行する回路となる復号回路構成情報を読み出し復号回路をＦＰＧＡ内に展開する（ステップ３）。次に、回路情報が暗号化された回路情報暗号化データを読み出し、ＦＰＧＡ内に展開された復号回路に入力する（ステップ４）。そこで、ＦＰＧＡ内に備えている、ＲＯＭに格納した回路情報を暗号化する際に使用した暗号化鍵と同一の鍵データを復号回路に入力し（ステップ５）、回路情報を復号する（ステップ６）。復号した回路情報は、ＳＲＡＭに記憶して（ステップ７）ＦＰＧＡの所望の回路を構成し、ＦＰＧＡとして機能する（ステップ８）。

【００１１】次に、本発明に基づいたＦＰＧＡを設計する際に必要なＲＯＭへの回路情報書き込み手順について説明する。図３は、本発明に係るＲＯＭへの回路情報書き込み手順について説明した流れ図である。同図を説明すると、ＦＰＧＡに持たせる必要な機能を具体化する回路設計を行い（ステップ１）、設計した回路に対応する

5

回路図、或いは、ハードウェアディスクリプションランゲージ（以降、ＨＤＬと称す）を用いて回路の機能レベルを論理記述したものを作成する（ステップ２）。更に、前記回路図或いはＨＤＬによる記述をもとに、回路を接続する素子間の接続関係や素子の電気的特性を記述したテキストファイルであるネットリストを作成し（ステップ３）、更に、ＦＰＧＡに格納する鍵データと同一の鍵データによりネットリストを暗号化する（ステップ４）。次に、暗号化データを暗号化されていないデータに復号するための復号回路の回路図或いはＨＤＬによる記述を作成し（ステップ５）、この回路図、或いは、ＨＤＬによる記述をもとにネットリストを作成する（ステップ６）。最後に、ステップ４により作成した暗号化したネットリスト及びステップ６により作成したネットリストをＲＯＭに書き込む（ステップ７）。このようにして、回路情報を書き込んだＲＯＭを用意し、電源投入時にＦＰＧＡにデータを出力させる。

【００１２】

【発明の効果】本発明は上述したように、ＦＰＧＡの回路情報保護のために暗号化技術を取り入れたものであり、ＳＲＡＭ方式を採用したＦＰＧＡに必要な回路情報を読み出すＲＯＭの内容を保護し、不正コピーを防止する上で大きな効果を発揮することが可能となる。　＊

6

＊【図面の簡単な説明】

【図１】本発明に係るＦＰＧＡの回路情報保護方法の一実施例を示す構成図であり、（ａ）にブロック構成例を、（ｂ）に処理の流れ図を示す。

【図２】共通鍵方式による暗号化処理の流れを示す。

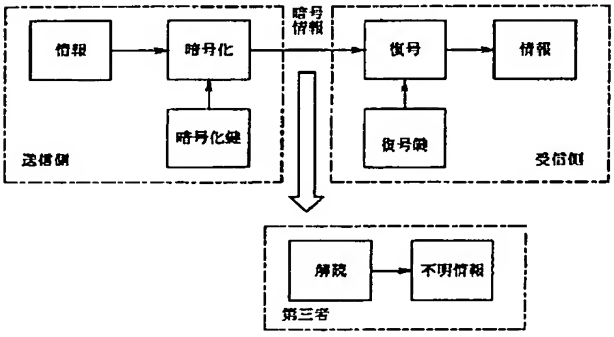
【図３】本発明に係るＲＯＭへの回路情報書き込み手順について説明した流れ図である。

【図４】従来から用いられているＳＲＡＭ方式ＦＰＧＡのチップ構成例を示す。

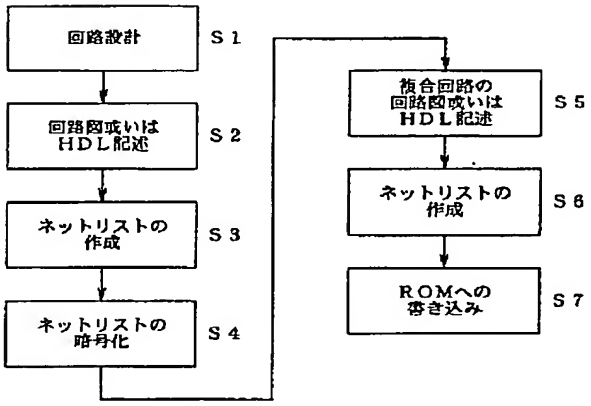
【符号の説明】

１・・ＦＰＧＡチップ、
２・・入出力ブロック、
３・・論理ブロック、
４・・スイッチマトリックス、
５・・１ビットＳＲＡＭセル、
６・・ＦＥＴトランジスタ、
７・・ＲＯＭ、
８・・ＦＰＧＡ、
９・・復号回路構成情報格納部、
１０・・回路情報暗号化データ格納部、
１１・・制御部、
１２・・鍵データ格納部、
１３・・回路情報記憶用ＳＲＡＭ

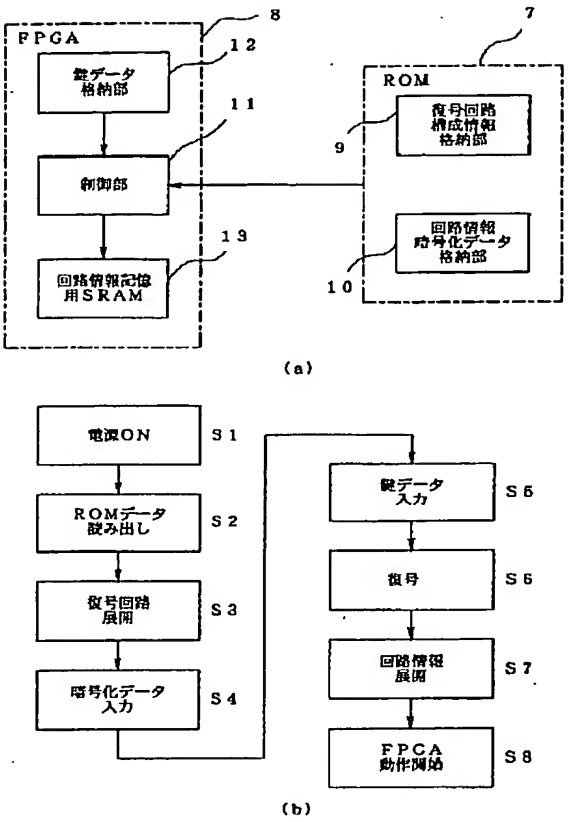
【図２】



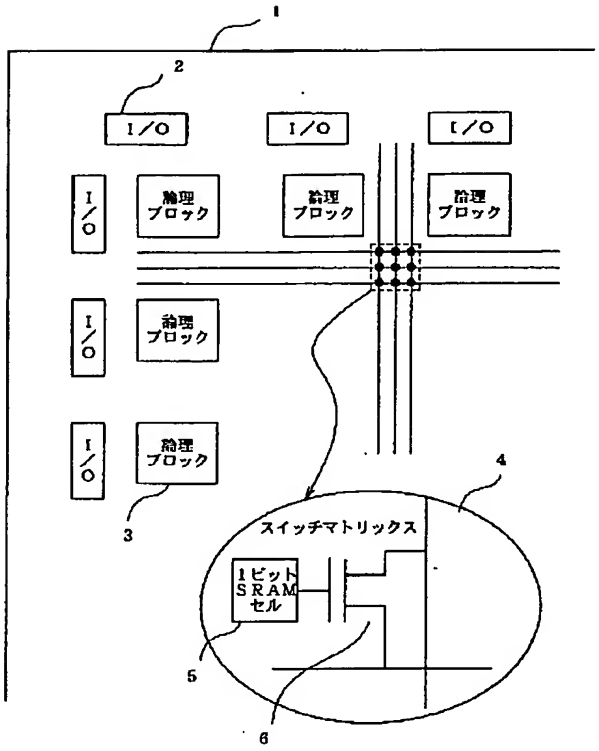
【図３】



【図１】


FPGA
8
12
鍵データ格納部
11
制御部
13
回路情報記憶用SRAM
7
ROM
9
復号回路構成情報格納部
10
回路情報暗号化データ格納部
(a)
電源ON
S1
ROMデータ読み出し
S2
復号回路展開
S3
暗号化データ入力
S4
鍵データ入力
S5
復号
S6
回路情報展開
S7
FPGA動作開始
S8
(b)

【図４】


1
2
I/O
I/O
I/O
I/O
論理ブロック
論理ブロック
論理ブロック
I/O
論理ブロック
I/O
論理ブロック
3
4
スイッチマトリックス
1ビットSRAMセル
5
6